**Rangkuman Modul 1 : Cyber Security Fundamental**

Pada modul ini membahas konsep basic dari cyber security, serta tujuan dan prinsip pada cybersecurity. Selain itu modul ini juga menjelaskan apa yang perlu diamankan pada system.

Pada modul ini berdasarkan sudut pandang dari seorang IT Manager

Internet merupakan jaringan besar dimana terdapat banyak system dan jaringan yang saling terhubung. Sistem yang berbeda dapat saling berinteraksi dengan protocol standar yang mana tiap system dapat saling bertukar informasi satu dengan yang lainnya. Bersamaan dengan ini terdapat juga resiko pada keamanan data.

Jika menyangkut internet, harus memikirkan 3 aspek utama, yakni :

1. Efficiency
2. Reliability
3. Security

Data-data perusahaan sangat berharga, dan merupakan asset bagi suatu perusahaan. Maka data ini perlu diamankan, data dan informasi yang perlu diamankan seperti :

1. Laporan Internal
2. Data Transaksi
3. Data Pelanggan
4. Desain Produk atau rahasia perusahaan

Setelah mengetahui data yang perlu diamankan, perlu tahu beberapa ancaman yang mengancam data tersebut, diantaranya ialah :

1. Unauthorized Modification : Perubahan data yang dilakukan oleh orang yang tidak punya akses
2. Unauthorized Access : Akses informasi oleh orang luar
3. Loss of information : Kehilangan data terjadi ketika informasi berharga atau sensitif di komputer hilang atau tersebar karena pencurian, kesalahan manusia, virus, malware, atau kegagalan daya. Ini juga dapat terjadi karena kerusakan fisik atau kegagalan mekanis atau peralatan suatu bangunan

Data yang perlu diamankan terbagi menjadi 2 golongan data :

1. Data at Rest : Data yang sudah tidak aktif, seperti backup dari aplikasi yan\g sudah off
2. Data Motion : Data yang masih aktif bergerak dan masih dilakukan pengeditan.

Setelah mengetahui data yang perlu diamankan, kita perlu mengetahui tujuan dari pengamanan data tersenbut. Tujuan dari cyber security ini bisa di singkat dengan CIA, dengan detail sebagi berikut ;

C » Confidentally : dibatasi dari unathorized akses

I » Integrity : menjaga keakuratan dan kelengkapan informasi (data tidak dapat dibuat, diganti, atau dihapus tanpa proses otorisasi.)

A » Availability : ketersediaan, informasi bisa diakses oleh orang yang memiliki otoritas kapanpun dan tanpa delay

Studi Kasus :

Contoh penerapan CIA pada webmail

C : Credential hanya diketahui oleh pemilik email, data pasword disimpan dengan enkripsi yang kuat dan tidak mudah untuk di decript

I : Email tidak diubah dari bentuk aslinya

A : Email service harus selalu aktif

Setelah mengetahui tujuan dari cyber security, modul ini membahas kerentanan yang mengancam data. Kerentanan-kerentanan yang mengancam data ialah threat, vulnerabilities, dan risk.

* Threat/ancaman bisa disebabkan secara sengaja ataupun kecelakaan, macam2 jenis ancaman adalah :
* Natural Threat (bencana alam)
* Environmental (Lingkungan/ aspek negatif dari aktivitas manusia) = power failure, polusi, liquid leakage (kebocoran / kena air)
* Human : kelalaian, unathorize access (hancking), virus
* Vulnerability / kerentanan merupakan kekurangan atau kelemahan pada keamanan prosedur system, design, pengimplementasian, dan control dari dalam yang dapat menyebabkan pelanggaran keamanan atau kekerasan pada peraturan keamanan system.
* Risk / resiko adalah hasil yang didapatkan dari kegiatan ancaman dan potensi dari kerentanan informasi yang memberikan dampak pada organisasi

Setelah mengetahui kerentanan data, pada modul ini diberikan cara menanggulangi kerentanan tersebut. Yakni

* Policy & Procedure (Membuat Kebijakan & Prosedur) : Tujuan dari kebijakan dan prosedur adalah untuk membuat semau orang waspada terhadap pentingnya keamanan. Jadi tiap system didefinisikan role dan apa yang bisa dilakukan serta bagian mana saja yang bisa diakses.
* Technical : Tujuan dari technical security control ntuk menangkal serangan luar, seperti virus, ataupun peretas. Yang dilakukan adalah dengan memasang firewall, ids, dan anti virus.
* Phisical : Tujuan dari pengamanan fisik adalah untuk mencegah pencurian, dan penggunaan alat tanpa izin. Yang bisa dilakukan ialah memasng cctv, dan mengamankan dengan kunci

Untuk menerapkan cybersecurity terdapat 2 prinsip yang perlu diingat, yakni

* Principle of Weakest Link : Attacker selalu mencari jalan termudah untuk meretas
* Principle of Least Privilage : Pengguna untuk mengakses perlu izin akses atau authorization

**Perbedaan Nginx dan Apache**

1. Penanganan Traffic

Apache : Apache memproses traffic dengan multi-processing modules (MPM)

Nginx : Web server ini memproses traffic menggunakan algoritma yang bersifat asinkron, non-blocking, dan event-driven

1. Pemrosesan Konten Dinamis

Apache : Apache bisa memproses konten dinamis tanpa bantuan software tambahan. Hal ini berkat adanya modul yang bisa Anda pasang dan lepas sesuai kebutuhan.

Nginx : Web server ini bergantung pada adanya software tambahan untuk memproses konten dinamis

Modul 2 : Cyber security in organization

Mengapa organisasi perlu keamanan?

Seperti yang kita pelajari di module 1, organisasi perlu mengamankan asset informasi mereka,

Alasan utama adalah, ancaman dapat mengeksplitasi vulnerabilities atau kerentanan yang dapat membahayakan dan mengganggu aktivitas bisnis

Untuk mengatasi ancaman api, organisasi meletakkan detector asap, dan alarm di lokasi strategis, melakukan pelatihan Ketika terjadi kebakaran, dan membeli asuransi. Sama akan hal itu, organisasi harus mengidentifikasi resiko keamanan dan memanage hal tersebut.

**Beberapa tipe serangan yang mempengaruhi bisnis**

Sebelum kita mulai mengidentifikasi celah keamanan, ada baiknya untuk memagami pengaruh kecelakaan keamanan pada organisasi.

Kecelakaan keamanan dapat mempengaruhi bisnis dalam berbagai macam:

* Database server down karenaq serangan DDoS (Distribute Denial of Service)

Operasional bisnis yang terganggu dengan serangan ini berhubungan ke supplier, kegagalan infrasruktur, etc

* Perlu waktu untuk memulihkan dari infeksi malware

Tentunya ini akan menambah pengeluaran

* Perusahaan bisa di denda oleh pemerintah karena pelanggaran informasi customer

Tidak dapat menyediakan servis sesuai kontrak, atau tidak mampu mematuhi peraturan

* Security incident menyebabkan customer menganggap bahwa perusahaan tidak serius mengamankan data customer

Mempengaruhi image perusahaan

**Managing Risk**

Perusahaan harus menginteifikasi dan mengelola resiko yang dapat mengganggu aktivitas perusahaan



Sekali resiok telah teridentifikasi dan dinilai dalam jangka waktu atau kemungkinan tertentu, perusahaan dapatt memilih,

* Mitigate

Memitigasi resiko dengan menerapkan control keamanan

* Transfer

Mentransfer resiko untuk dihanle oleh pihak ketiga, seperti asuransi dll.

**Meningkatkan kesiapan keamanan cyber**

* Menyadari tingkat dan kemungkinan resiko memungkinkan perusahaan lebih proaktif dan siap
* Pendekatan komprehensif untuk manajemen resiko harus melibatkan pihak di seluruh organisasi untuk meningkatkan kualitas pengambilan keputusan untuk mengelola resiko
* Upaya ini akan membutuhkan organisasi untuk menginvestasikan sumber daya (yaitu uang, waktu, dan personel) dan mengembangkan program keamanan siber yang komprehensif.
* Pada akhirnya top management bertanggung jawab untuk memastikan keamanan organisasi

1. Denial of Service Attack

Pada dasarnya serangan DoS dikirim melalui jaringan. Satu tekniknya adalah dengan mengirimkan banyak paket jaringan yang melampaui pemrosesan server atau jaringan.

Perusahaan yang memiliki layanan servis internet seperti website, dns, dan mail server, ini rentan terhadap serangan ini

1. Malware

Malware adalah malicious software (perangkat lunak berbahaya), seperti, virus, work, rootkits, backdoors, trojan

Pengguna komputer tertipu untuk menjalankan malware ini, Atau pembuat malware mengeksploitasi kerentanan perangkat lunak yang ada, setelah dijalankan pada sistem, ia akan membawa payload berikut :

* Merekam apa yang diketik pengguna
* Mengirimkan informasi (seperti file, database)
* Mengenkripsi file dan meminta uang tebusan (ransomware)

1. Identify Theft

Mengakses system menggunakan credential adalah hal yang normal

Identify theft terjadi Ketika penyerang mencuri identitas user, jadi mereka seolah-olah menjadi user tersebut dan mendapatkan akses ke system

Cara identify theft

* Phising
* Malware (menginstall malware (keylogger) untuk mencuri kredensial login)

1. Web Defacement

Perusakan web, web perusahaan biasanya memberikan informasi dan servis pada customer mereka. Web defacement terjadi Ketika konten website di ubah oleh penyerang. Itu bisa menyebabkan kerentanan pada web server atau cms. Dan menyebabkan unavailable service yang mempengaruhi reputasi perusahaan

Bagaimana memitigasi resiko serangan cyber?

It is said that in security there is no silver bullet or one single solution that will prevent or make the security problem go away (dikatakan bahwa dalam keamanan tidak ada peluru perak atau satu solusi tunggal yang akan mencegah atau menghilangkan masalah keamanan).

Untuk mengatasi resiko yang telah disebutkan sebelumny, kita harus menerapkan control pada beberapa level :

* Technical Control to detect & prevent

Firewall, spam filter, ids (intrution detection system), dan antivirus

* Education and training of our employees

Khususnya Ketika berkaitan dengan phising dan bagaimana membuat apliaksi web lebih aman

* Ensuring that network provides have capablitis to support us when we are under attack

(Memastikan bahwa menyediakan kemampuan untuk mensupport ketika terjadi serangan)

**Modul 3 : Cyber Security Control**

Countermeasure : Dalam keamanan, penanggulangan juga disebut sebagai perlindungan, kontrol keamanan, atau hanya control

Countermeasure berarti melakukan managing risk, seperti

* Policies and procedures
* Guidelines
* Practices or organizational structure

Dapat bersifat administratif, manajemen teknis, atau hukum

**Cyber security framework atau standard**

Kerangka kerja atau standar keamanan adalah serangkaian proses terdokumentasi yang digunakan untuk menentukan kebijakan dan prosedur di sekitar implementasi dan manajemen berkelanjutan dari kontrol keamanan adalah lingkungan perusahaan 

Beberapa framework cyber security yang populer

* ISO 27000 series (Information security management system)

ISO 27000 adalah bagian dari ISO/IEC Information Security Management System (ISMS) standards

* NIST Cyber Security Framework
* Payment Card Industry data Security Standard (PCI DSS)
* CIS Critical Security Control

**Security Policies**

kebijakan keamanan pada dasarnya menggambarkan apa yang harus dilakukan untuk melindungi organisasi dan aset informasinya. yang biasanya berupa dokumen tertulis yang mencakup bidang-bidang utama seperti :

* backup plan
* it asset policies
* password policies
* internet policies

kebijakan keamanan :

Sangat penting bahwa kebijakan keamanan dibagi dengan setiap pemangku kepentingan sehingga mereka menyadari tanggung jawab mereka dan harapan organisasi.

**Firewalls**

Fireall mencegah unauthorized access ke computer atau jaringan. Biasanya firewall dipasang pada batas antara dua jaringan. mereka bisa berupa perangkat keras atau perangkat lunak yang berjalan di komputer yang bertindak sebagai gateway

Host-based firewall adalah software yang berjalan di device enduser untuk mengamankan device tersebut

Yang akan dilakukan firwall :

* Inspect traffic berdasartkan aturan, dan akan menentukan untuk blok atau mengijinkan. Dan ini juga berguna untuk membatasi akses ke Sebagian system atau serviced
* Menyaring lalu lintas berdasarkan alamat sumber dan tujuan atau nomor port, jenis lalu lintas jaringan atau atribut jaringan

**Anti Malware**

Software anti malware dapat melindungi dari virus dan malware lainnya termasuk trojan, ransomware, worms, and spyware

Sebagaimana malware berevolusi sangat cepat, penting untuk memastikan bahwa anti malware memiliki infromasi terbaru untuk efektifitas deteksi.

**Vulnerability Management**

Manajemen kerentanan adalah praktik penting untuk mengidentifikasi klasifikasi, remediasi, dan mitigasi kerentanan.

Keharusan

Ini penting karena terkadang, kerentanan ditemukan dalam perangkat lunak atau firmware yang memungkinkan musuh mendapatkan akses tidak sah ke jaringan atau data

Contoh : menerapkan patch atau pembaruan secara tepat waktu adalah contoh hasil dari proses ini

**IDS (Intrution Detection System)**

IDS adalah device atau software yang memonitor jaringan dan system dari malicious activity



Fungsi IDS :

* Menginvestigasi paket dan melihat atribut yang mengandung malicious activity atau policy activity. Aktivitas ini akan tercatat dan menginformasikan admin untuk penanganan lebih lanjut
* Can be network or host based
* Hanya berfungsi sebagai detector atau Intrusion Prevention System (IPS) untuk memblokir atau menghentikan malicious activity

**Encription**

Encription adalah Langkah keamanan yang mengenkripsi file system, network transaction, removable media adan email. Data dan infrormasi yang dienkripsi hanya bisa diakses dengan kunci yang tepat atau password

* Untuk penanggulangan, enkripsi penting untuk melindungi atau mengurangi dampak dari kebocoran data dan pencurian
* Di organisasi, akan menemukan enkripsi yang serind dipakai di protocol jaringan (ssh, https, vpns,) dan email (pgp/smime)

**2FA**

2FA adalah metode autemntikasi yang mengkonfirmasi user menggunakan 2 kompone yang berbeda.



**Security Audit**

Audit keamanan adalah penilaian teknis terukur dari suatu sistem atau aplikasi.

Cara melakukan audit kemanana adalah sebagai berikut

* Interviews
* Security Vulnerability Scans
* Analyzing physical access to the system

**Incident Responsce & Handling**

Untuk menyiapkan respon dan penanganan kecelakaan keamanan, penting untuk memimalkan dampak dari kebobolan keamaman atau penyerangana, dan pemulihat yang cepat. Prosedurnya adalah sebagai berikut :

* Mendeteksi type dari security incident
* Menghapus akar masalah dari insiden
* Memulihkan ke sebelum terjadinya insiden
* Review dan pelajari dari insiden untuk peningkatan di masa depan

Beberapa organisasi meiliki team yang menangani keamanan, mereka mempunyai skill untuk performing logs analysis, malware investigation, and digital forensics. CSIRT / tim keamanan beberapakali perlu bekerja dengan pihak external seperti firma hukum, operator jaringan, atau Lembaga pemerintah.

**Education & Training**

* Memiliki kesadaran keamanan itu penting untuk mengamankan organisasi
* Security tidak bisa berhasil tanpa support dari semua stakeholder di organisasi
* Staff perlu waspada pentingnya keamanan peraturan dan pencegahan keamanan pada role mereka dan responnya.

Hal ini dapat dicapai dari campaign security awareness, training, or desktop exercise

**Kesimpulan**

* Banyak pencegahan yang dapat digunakan tergantung dari bagaimana dan apa yang mau dicapai
* Penting untuk memhami bahwa semua elemen penanggulangan harus bekerja bersama untuk lebih efektif
* Pada beberapa kasus, kita menaruh banyak keamanan di layer untuk memperkuat keamanan

**Modul 4**

Respon yang harus dilakukan tiap bagian

1. Network Enginer

Network enginer bertanggung jawab umtuk mengimplementasi, merawat, mensupport, dan mendesign komunikasi jaringan dengan organisasi atau antar organsasi

Goal : memastikan ketersediaan infrastruktur jaringan untuk memberikan kinerja maksimal bagi penggunanya

User :

* Staff
* Client
* Customer
* External supplier

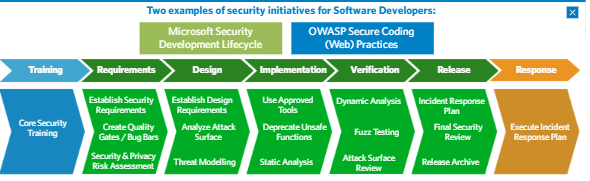
Yang harus dilakukan oleh network engineer

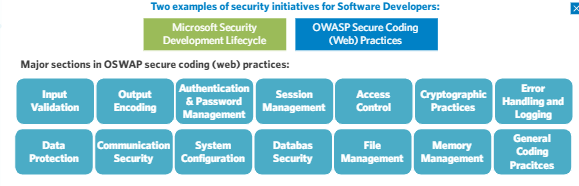
* Mengkonfigurasi peralatan jaringan (router, firewall, ids) dengan aman
* Mengamankan system jaringan dengan menetapkan kebijakan, dan mendefinisikan, dan monitoring akses
* mensupport firewall sejalan dengan kebijakan keamanannya
* Memhamai security issues di berbagai lapisan jaringan

1. Software Developer

SD bertanggung jawab untuk menulis coding program sesuai requirement







1. Security Analyst

Security analyst bertanggung jawab untuk merencanakan dan mengimplementasikan pengukuran keamanan untuk mengamankan system computer, jaringan, dan data

Mereka diharapkan untuk tetap uptodate pada trend kemaanan termasuk Teknik penyerangan. Untuk mengantisipasi pelanggaran keamanan

* Developing capabilities to detect threats and policy breach

Mengembangkan kemampuan untuk mendeteksi ancaman dan pelanggaran kebijakan

* Creating, testing, and implementing disaster recovery plan

Membuat, menguji, dan menerapkan rencana pemulihan bencana

* Performing risk and vulnerability assessment

Melakukan penilaian risiko dan kerentanan

Skill yang dibutuhkan security analist

* Memiliki pemahaman yang bagus terkain jaringan, os, dan security control
* Problem solving
* scripting

1. Digital forensic analyst

Digital Forensic analyst memulihkan dan memeriksa data dari komputer dan perangkat penyimpanan elektronik lainnya yang digunakan, data tersebut sebagai bukti dalam penyelidikan atau dalam tuntutan pidana

**Pentingnya analis forensik digital**

Keahlian mereka penting dalam membantu memahami akibat dari keamanan atau pelanggaran dunia maya. Hal ini terkadang memerlukan informasi korelasi yang diperoleh dari log, aliran jaringan, dan sumber daya lainnya

**Skill yang dibutuhkan**

* Pemahaman yang kuart mengenai cara kerja OS (memory, file system, dan registry)
* Familiar dengan specialized tools

1. Security Auditor

Security Auditor bertanggung jawab untuk memastikan bahwa security plan and control diimplementasikan dengan benar.

Mereka membantu untuk mengidentifikasi practise yang tidak sesuai terkait kebijakan yang ada / standard keamanan. Mereka juga akan mendiskusikan kemungkinan untuk peningkatan kepada stakeholder terkait

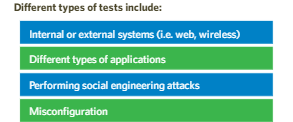
Skill yang dibutuhkan :

* berpengalaman dalam standar keamanan
* pemahaman teknis yang kuat tentang sistem yang diaudit
* Perhatian terhadap detail

1. Penetration Testers

Pen Tester bertanggung jawab untuk mengetes semua keamanan organisasi dengan mencari kelemahan pada jaringan, software, system atau staff/

Mereka biasanya bekertja dekat dengan stakeholder yang lain untuk memastikan cleah yang mereka temukan sudah diperbaiki



Skill yang dibutuhkan :

* pemahaman yang baik tentang keamanan
* latar belakang teknis yang kuat di berbagai bidang termasuk jaringan, os, protokol, dan pemrograman

1. Eksekutif level

CEO memiliki peran besar pada semua implementasi keamanan

* Memastikan keamanan tersedia, sumber daya yang cukup dialokasikan untuk keamanan, dan pahami kemampuan pertahanan dunia maya organisasi
* Tunjukkan kepemimpinan dengan memberi contoh, keamanan dunia maya adalah salah satu prioritas utama dan faktor penentu keberhasilan bagi organisasi



Learning & Certification

Security Management

* CISP (Certified Information System Security Professional)
* CISM (Certified Information Security Manager)

Specialized Courses

* EnCE (EnCase Certified Examiner)
* SANS GIAC Certified Incident Handler

Online Courses

* MitopenCourseware
* Coursera

Specialized domains in cyber security

* Malware
* Digital Fornsik
* Incident Response